UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,651	01/28/2002	Steven M. Blumenau	10830.0033.DVUS01	5520

27927 7590 06/17/2005

RICHARD AUCHTERLONIE
NOVAK DRUCE & QUIGG, LLP
1000 LOUISIANA
SUITE 5320
HOUSTON, TX 77002

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,651	BLUMENAU, STEVEN M. ET AL	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In view of the Appeal Brief filed on 3/23/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. **Claims 1 - 12** are pending. Independent Claims are **1, 7, 12**.

Response to Arguments

3. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

3.1 In light of applicant's arguements that the combination of Best, Rigal and Little does not addressing limitations present within pending claims, applicant is

henceforth reminded that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Furthermore, in response to an applicant's arguments against a reference individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Examiner respectfully upholds the rejection of all claims, due to the fact that the combination of Jones, Best, Rigal and Little discloses the claims and limitations of applicant's invention.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 3 - 7, 9, 12,** are rejected under 35 U.S.C.103(a) as being unpatentable over **Jones et al.** (US Patent No. 6,088,800) in view of **Best** (US Patent No. 4,465,901) and further in view of **Rigal** (US Patent No. 5,881,155).

Regarding Claims 1, 7, Jones discloses the art of cryptographic microprocessor authentication protocol, which resides in an electronic circuit chip comprising:

a) a memory for storing information defining an encryption procedure assigned to the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 5, lines 25-28; col. 3, lines 48-54: encryption chip, programmable, memory for storage of encryption program instructions)

b) at least one input to the electronic circuit chip for writing, to the memory, the information defining the encryption procedure assigned to the electronic circuit chip, and for receiving data to be encrypted by the encryption procedure assigned to the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 6, lines 6-8: encryption chip, input means for encryption process)

c) encryption circuitry for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data (see Jones col. 3, lines 33-36; col. 3, lines 48-54: encryption chip, memory for encryption program instructions);

d) at least one output from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry (see Jones col. 3, lines 33-36; col. 6, lines 14-18: encryption chip, output means for transmission of encrypted data);

e) wherein the electronic circuit chip is constructed so that the information defining the encryption procedure assigned to the electronic circuit chip cannot be read from the memory from any output of the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 6, lines 20-24: encryption chip, host computer only interface for program load)

Jones does not specifically disclose an encryption chip constructed such that information cannot be recovered by probing or a metal shielding over the memory. However, Best discloses:

f) wherein the electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly. (see Best col. 16, lines 42-50: *"If the enciphered program is small enough it may be stored in ROM in cipher or transposed form on the crypto-microprocessor chip to prevent a pirate from reading the program from a photographic enlargement of the chip or by probing an easily found internal bus ..."*; col. 18, lines 26-37)

g) metal, oxide and semiconductor (MOS) materials in chip composition, but does not specifically mention a metal shielding layer over the memory. However, Rigal in analogous art discloses a metal shielding layer. (see Best

Figures 5 and 6 ; col. 6, lines 30-37: *"....Guard ring 50 is a metallic layer used to electrically isolate the protected chip from external electrical influences. Its specific dimensions are not of particular importance. For example, guard ring 50 can be formed at the periphery of the protected chip 10 and on a surface of the protective chip 20 ... ")*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to enable chip construction so it is impossible to recover information by probing as taught by Best, and to enable a metallic layer over EEPROM as taught in Rigal. One would have been motivated to employ Best in order to optimize execution of encryption programs while maintaining the security of encryption programs, and to employ the metallic layer in Rigal in order to reduce tampering capability, so that the information stored within memory cannot be read by visual inspection or probing and the information can also be resistant to interference, which enhances protection of the confidential information stored within the chip.

Regarding Claims 3, 9, Jones discloses a programmable encryption chip. (see Jones col. 3, lines 33-36; col. 3, lines 41-51; col. 3, lines 38-41: a programmable encryption chip utilizing memory) Jones does not disclose a read only and electrically erasable memory. However, Best discloses the electronic circuit chip, wherein the memory is an electrically erasable and programmable read-only memory. (see Best col. 14, lines 3-7: "*... electrically alterable read-only memory then a battery is not needed and loading circuit 76 would be changed accordingly ... "*; col. 20, lines 46-61)

Regarding Claim 4, Jones discloses the electronic circuit chip, wherein said encryption circuitry includes a microprocessor for computing the encrypted data. (see Jones col. 3, lines 33-36; col. 3, lines 38-41: encryption chip, processor to perform encryption techniques based on programming)

Regarding Claim 5, Jones discloses the electronic circuit chip as claimed in claim 4, wherein the microprocessor is constructed to execute an encryption program stored in the memory, and the encryption program defines the encryption procedure assigned to the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 3, lines 38-41: encryption chip, execute instruction for programmed algorithm)

Regarding Claim 6, Jones discloses the electronic circuit chip as claimed in claim 4, wherein said microprocessor is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 6, lines 30-43: encryption chip, public key encryption algorithms utilized)

Regarding Claim 12, Jones discloses an electronic circuit chip comprising:

a) - g) These limitations encompass the same scope of the invention as that of the claim 1. a - g, therefore these limitations are rejected for the same reason as the claim 1. a - g.

i) Jones discloses wherein the microprocessor is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip. (see Jones col. 3, lines 33-36; col. 6, lines 30-43: encryption chip, public key encryption algorithms utilized)

Neither Jones nor Best disclose a metal shielding over the encryption chip memory. However, Rigal discloses:

h) the electronic circuit chip is a semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory (*EEPROM)* , and the *metal* shielding layer over the memory is an upper layer of metal on the electronic circuit chip; (see Rigal, col. 4, lines 53-62, *".....provided with an electrically erasable memory (EEPROM or flash EPROM), a volatile memory (RAM) and encryption capabilities."* and Rigal, FIGS. 5 and 6, and col. 6, lines 30-37: *"....Guard ring 50 is a metallic layer used to electrically isolate the protected chip...)*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Jones to enable the usage of a semiconductor chip as taught by Best, and to enable the metal shielding layer over the EEPROM as taught in Rigal. One would have been motivated

to employ Best in order to optimize execution of encryption programs while maintaining the security of encryption programs, and to employ the type of chip as Rigal in order to make a reliable and efficacious solution for enhanced security against an unlawful attempt to gain access to data stored in a security device.

6. **Claims 2, 8, 10, 11** are rejected under 35 U.S.C.103(a) as being unpatentable over **Jones-Best-Rigal** as applied to claims 1, 7 above and further in view of **Little et al.** (U.S. Patent No. 5,998,858).

Regarding Claims 2, 8, Jones discloses an encryption chip. Jones does not specifically disclose a semiconductor IC chip. However, Best discloses the electronic circuit chip with a type of semiconductor integrated circuit chip (see col. 18, line 66 - col. 19, line 12), however, Best's chip is not *monolithic* semiconductor integrated circuit chip. Little discloses a *monolithic semiconductor chip* (see col. 18, lines 26-37: *"The electronic data module 100, ... is designed to hermetically house a monolithic semiconductor chip 135 that may comprise a host of circuit elements such as memory, microprocessors, multiplexing circuitry and electrostatic discharge protection circuitry.")*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Best with a monolithic semiconductor chip as taught in Little. One would have been motivated to substitute the monolithic semiconductor chip

in Little in order to enhance detection associated with an unlawful attempt to gain access data stored in the chip.

Regarding Claims 10, 11, Jones disclose an encryption chip. Jones does not disclose semiconductor chip. However, Best discloses the electronic circuit chip as claimed in claims 1, 7, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, (see Little col. 18, lines 26-37) the memory is an electrically erasable and programmable read-only memory, (see Best col. 14, lines 3-7; see Rigal col. 4, lines 53-62) and the metal shielding layer over the memory is an upper layer of metal (see Rigal col. 6, lines 30-37) on the electronic circuit chip. (see Best col. 16, lines 42-46)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Best with a metallic layer over EEPROM as taught in Rigal and monolithic semiconductor chip as taught in Little. One would have been motivated to combine the metallic layer in Rigal and monolithic chip in Little in order to make an effective chip for reducing tampering capability, so that the information stored in the memory cannot be read by visual inspection or probing, which enhances protection of the confidential information stored in the chip.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
June 12, 2005

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER